

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-252323

(43)Date of publication of application : 22.09.1997

(51)Int.Cl.

H04L 12/56

G09C 1/00

H04L 9/32

H04L 12/22

(21)Application number : 08-344862

(71)Applicant : SONY CORP

(22)Date of filing : 25.12.1996

(72)Inventor : TERAOKA FUMIO

(30)Priority

Priority number : 08 3009

Priority date : 11.01.1996

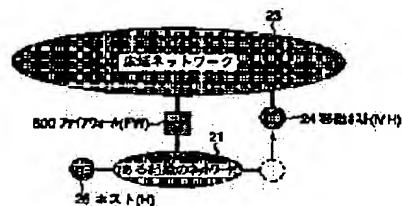
Priority country : JP

(54) COMMUNICATION SYSTEM AND COMMUNICATION EQUIPMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To improve the security by allowing only a mobile host pertaining to its own organization to access the its own organization externally in the communication based on a virtual internet protocol.

SOLUTION: A fire wall 300 and a mobile host 24 store respectively the same key information and the same arithmetic operation method, and when the mobile host 24 moves from a network 21 and connects to a broad area network 23 and sends a packet to a host 25, the host 24 confirms authentication information based on the key information and information included in a header of the packet and sends packet including it in its header information. The fire wall 300 relays a packet when the authentication information calculated similarly based on the key information and the header information of the packet from the mobile host 24 is matched with the authentication information included in the header information.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-252323

(43) 公開日 平成9年(1997)9月22日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 12/56		9466-5K	H 0 4 L 11/20	1 0 2 A
G 0 9 C 1/00	6 6 0	7259-5 J	G 0 9 C 1/00	6 6 0 E
H 0 4 L 9/32			H 0 4 L 9/00	6 7 5 A
12/22		9466-5K	11/26	

審査請求 未請求 請求項の数 8 O L (全 12 頁)

(21) 出願番号 特願平8-344862

(22) 出願日 平成8年(1996)12月25日

(31) 優先権主張番号 特願平8-3009

(32) 優先日 平8(1996)1月11日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 寺岡 文男

東京都品川区北品川6丁目7番35号 ソニー株式会社内

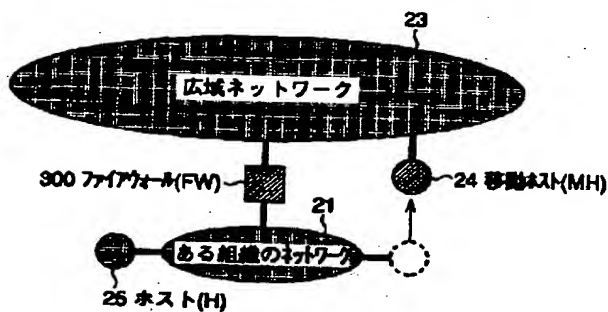
(74) 代理人 弁理士 稲本 義雄

(54) 【発明の名称】 通信システムおよび通信装置

(57) 【要約】

【課題】 仮想インターネットプロトコルに基づいた通信において、自組織に属する移動ホストだけが外部から自組織内にアクセスすることができるようにし、セキュリティを向上させる。

【解決手段】 ファイアウォール300と移動ホスト24は、同一の鍵情報と演算方法をそれぞれ記憶し、移動ホスト24がネットワーク21から移動し、広域ネットワーク23に接続し、ホスト25にパケットの送信を行うとき、鍵情報とパケットのヘッダに含まれる情報に基づいて認証情報を演算し、パケットのヘッダ情報に含ませて送信する。ファイアウォール300は、鍵情報と移動ホスト24からのパケットのヘッダ情報から同様にして演算した認証情報と、ヘッダ情報に含まれる認証情報とが一致する場合、そのパケットを中継する。



【特許請求の範囲】

【請求項1】 第1のネットワークと第2のネットワークが通信装置を介して接続され、前記第1のネットワークの送信局から前記第2のネットワークの受信局に送信されたパケットが、前記通信装置によって選択的に、前記第2のネットワークに中継される通信システムにおいて、

前記送信局は、

所定の鍵情報を記憶する第1の記憶手段と、

所定の演算方法を記憶し、前記第1の記憶手段に記憶された前記鍵情報と、前記受信局に送信すべきパケットのヘッダ情報に基づいて、前記演算方法に従って第1の認証情報を演算する第1の演算手段と、

前記第1の演算手段によって演算された前記第1の認証情報を前記パケットのヘッダ情報に含めて送信する送信手段とを備え、

前記通信装置は、

前記鍵情報を記憶する第2の記憶手段と、

前記演算方法を記憶し、前記第2の記憶手段に記憶された前記鍵情報と、前記送信局からの前記パケットのヘッダ情報に基づいて、前記演算方法に従って第2の認証情報を演算する第2の演算手段と、

前記送信局からの前記パケットのヘッダ情報に含まれる前記第1の認証情報と、前記第2の認証情報とを比較する比較手段と、

前記比較手段による比較結果に基づいて、前記パケットを前記第2のネットワークに中継するか否かを決定する決定手段とを備えることを特徴とする通信システム。

【請求項2】 前記パケットのヘッダ情報には、少なくとも前記送信局の位置を表す第1の情報と、前記送信局の位置に依存しない前記送信局を識別するための第2の情報とが含まれることを特徴とする請求項1に記載の通信システム。

【請求項3】 前記通信装置は、前記送信局の前記第2の情報を前記第1の情報に変換する変換手段をさらに備えることを特徴とする請求項1に記載の通信システム。

【請求項4】 前記第2のネットワークには、1または複数のサーバが接続され、

前記送信局から前記サーバに送信されたパケットは、前記通信装置の前記決定手段により、前記第2のネットワークへの中継が決定されたとき、前記第2のネットワークに接続された前記サーバに伝送されることを特徴とする請求項1に記載の通信システム。

【請求項5】 前記サーバは、メールサーバであることを特徴とする請求項4に記載の通信システム。

【請求項6】 複数のネットワークインタフェースを有し、前記ネットワークインタフェースの所定のものを介して受信した送信局からのパケットを、前記ネットワークインタフェースの他の所定のものを介して送信することにより、ネットワーク間でパケットの中継を行う通信

装置において、

前記ネットワークインタフェースを介して受信した前記送信局からの前記パケットに含まれるヘッダ情報が本物であるか否かを認証する認証手段と、

前記認証手段により、前記パケットに含まれる前記ヘッダ情報が本物であると認証されたとき、前記パケットが中継されるよう制御する制御手段とを備えることを特徴とする通信装置。

【請求項7】 前記認証手段は、所定の鍵情報および演算方法を記憶し、

前記ネットワークインタフェースを介して受信した前記送信局からの前記パケットに含まれる前記ヘッダ情報と前記鍵情報に基づいて、前記演算方法に従った所定の演算を行うことにより、所定の認証情報を演算し、前記認証情報と同一のものが前記パケットのヘッダ情報の中に含まれるか否かに基づいて、前記ヘッダ情報が本物であるか否かを認証することを特徴とする請求項6に記載の通信装置。

【請求項8】 前記送信局は、前記認証手段が記憶する前記鍵情報および演算方法と同一のものを記憶し、前記パケットのヘッダ情報に基づいて前記認証情報を演算し、前記認証情報を前記パケットのヘッダ情報に含めることを特徴とする請求項6に記載の通信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信システムおよび通信装置に関し、例えば、パケットのヘッダ情報に基づく認証機能を有し、通信のセキュリティを向上させ、外部から自組織内にアクセスすることができるようにした通信システムおよび通信装置に関する。

【0002】

【従来の技術】ルータは複数のネットワークインタフェースを有する装置であり、パケットの中継を行う。図9は、ルータの構成例を示すブロック図である。このルータ100においては、所定のネットワークインタフェース(network i/f) 1a乃至1cのいずれかより受信したパケットは、送信ネットワークインタフェース決定器(output network i/f selector) 2によって決定されたネットワークインタフェース1a乃至1cのいずれかより送信される。このネットワークインタフェースを決定する際には、経路表(routing table) 3が利用される。

【0003】また、外部と接続しているルータであって、所定の組織内のネットワークを守るために、外部からのパケットを選択的にこの組織に中継するルータを特にファイアウォールと呼ぶ。図10は、ファイアウォール200の構成例を示すブロック図である。上述したように、ファイアウォール200は、選択的にパケットの中継を行うルータであり、図9に示したルータ100に、パケットの選別を行う機能を有するパケット選別器

11が付加されている。

【0004】パケット選別器11は、パケットヘッダに含まれている送信ホストアドレス、受信ホストアドレス、およびプロトコルの種別等のヘッダ情報を用いてパケットの選別を行う。従って、所定のホストからのパケットだけを選択的にこの組織内に中継するようにすることができる。

【0005】

【発明が解決しようとする課題】しかしながら、これらのヘッダ情報の内容は正しいとは限らない。不正なユーザが、偽りのヘッダ情報を使用していることも考えられる。従って、不正なユーザがこの組織内にアクセスする可能性があり、通信のセキュリティが確保できない場合がある課題があった。

【0006】本発明はこのような状況に鑑みてなされたものであり、不正なユーザからのパケットを中継しないようにすることにより、ネットワークのセキュリティを向上させることができるようにするものである。

【0007】

【課題を解決するための手段】請求項1に記載の通信システムは、送信局は、所定の鍵情報を記憶する第1の記憶手段と、所定の演算方法を記憶し、第1の記憶手段に記憶された鍵情報と、受信局に送信すべきパケットのヘッダ情報に基づいて、この演算方法に従って第1の認証情報を演算する第1の演算手段と、第1の演算手段によって演算された第1の認証情報をパケットのヘッダ情報に含めて送信する送信手段とを備え、通信装置は、鍵情報を記憶する第2の記憶手段と、演算方法を記憶し、第2の記憶手段に記憶された鍵情報と、送信局からのパケットのヘッダ情報に基づいて、この演算方法に従って第2の認証情報を演算する第2の演算手段と、送信局からのパケットのヘッダ情報に含まれる第1の認証情報と、第2の認証情報とを比較する比較手段と、比較手段による比較結果に基づいて、パケットを第2のネットワークに中継するか否かを決定する決定手段とを備えることを特徴とする。

【0008】請求項6に記載の通信装置は、ネットワークインタフェースを介して受信した送信局からのパケットに含まれるヘッダ情報が本物であるか否かを認証する認証手段と、認証手段により、パケットに含まれるヘッダ情報が本物であると認証されたとき、パケットが中継されるよう制御する制御手段とを備えることを特徴とする。

【0009】請求項1に記載の通信システムにおいては、送信局において、第1の演算手段により、第1の記憶手段に記憶された鍵情報と、受信局に送信すべきパケットのヘッダ情報に基づいて、記憶している演算方法に従って第1の認証情報が演算され、送信手段により、第1の演算手段によって演算された第1の認証情報がパケットのヘッダ情報に含められて送信される。また、通信

装置において、第2の演算手段により、第2の記憶手段に記憶された鍵情報と、送信局からのパケットのヘッダ情報に基づいて、記憶している演算方法に従って第2の認証情報が演算され、比較手段により、送信局からのパケットのヘッダ情報に含まれる第1の認証情報と、第2の認証情報とが比較され、この比較結果に基づいて、決定手段により、パケットを第2のネットワークに中継するか否かが決定される。従って、通信装置が記憶している鍵情報および演算方法と同一のものを記憶している送信局からのパケットのみを、選択的に中継するようにすることができる。

【0010】請求項6に記載の通信装置においては、認証手段により、ネットワークインタフェースを介して受信した送信局からのパケットに含まれるヘッダ情報が本物であるか否かが認証され、制御手段により、認証手段によってパケットに含まれるヘッダ情報が本物であると認証されたとき、パケットが中継されるよう制御される。従って、ヘッダ情報が本物である場合にだけ、そのパケットを中継するようにすることができる。

【0011】

【発明の実施の形態】以下に、本発明の実施の形態を説明するが、その前に、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し、一例）を付加して、本発明の特徴を記述すると、次のようになる。

【0012】すなわち、請求項1に記載の通信システムは、第1のネットワーク（例えば、図1の広域ネットワーク23）と第2のネットワーク（例えば、図1のある組織のネットワーク21）が通信装置（例えば、図1のファイアウォール300）を介して接続され、第1のネットワークの送信局（例えば、図1の移動ホスト24）から第2のネットワークの受信局（例えば、図1のホスト25）に送信されたパケットが、通信装置によって選択的に、第2のネットワークに中継される通信システムにおいて、送信局は、所定の鍵情報を記憶する第1の記憶手段（例えば、図2の記憶部24a）と、所定の演算方法を記憶し、第1の記憶手段に記憶された鍵情報と、受信局に送信すべきパケットのヘッダ情報に基づいて、この演算方法に従って第1の認証情報を演算する第1の演算手段（例えば、図2の演算部24b）と、第1の演算手段によって演算された第1の認証情報をパケットのヘッダ情報に含めて送信する送信手段（例えば、図2の送受信部24c）とを備え、通信装置は、鍵情報を記憶する第2の記憶手段（例えば、図3の認証器31）と、演算方法を記憶し、第2の記憶手段に記憶された鍵情報と、送信局からのパケットのヘッダ情報に基づいて、この演算方法に従って第2の認証情報を演算する第2の演算手段（例えば、図3の認証器31）と、送信局からのパケットのヘッダ情報に含まれる第1の認証情報と、第

2の認証情報とを比較する比較手段（例えば、図3の認証器31）と、比較手段による比較結果に基づいて、パケットを第2のネットワークに中継するか否かを決定する決定手段（例えば、図3のパケット選別器11）とを備えることを特徴とする。

【0013】請求項3に記載の通信システムは、通信装置は、送信局の第2の情報を第1の情報に変換する変換手段（例えば、図3の経路表3）をさらに備えることを特徴とする。

【0014】請求項6に記載の通信装置は、複数のネットワークインタフェースを有し、ネットワークインタフェースの所定のものを通じて受信した送信局からのパケットを、ネットワークインタフェースの他の所定のものを通じて送信することにより、ネットワーク間でパケットの中継を行う通信装置において、ネットワークインタフェースを通じて受信した送信局からのパケットに含まれるヘッダ情報が本物であるか否かを認証する認証手段（例えば、図3の認証器31）と、認証手段により、パケットに含まれるヘッダ情報が本物であると認証されたとき、パケットが中継されるよう制御する制御手段（例えば、図3のパケット選別器11および送信ネットワークインタフェース決定器2）とを備えることを特徴とする。

【0015】なお、勿論この記載は、各手段を上記したものに限定することを意味するものではない。

【0016】以下、本発明の通信システムを適用したネットワークの一実施の形態について説明するが、その前に、本発明を実現するための仮想インターネットプロトコル（VIP: Virtual Internet Protocol）について簡単に説明する。

【0017】VIPとは、位置指示子（アドレス）と識別子とを明確に分離することにより、移動透過な通信（移動透過性）を実現するものである。

【0018】ここで、移動透過性とは、相手コンピュータの場所に拘らず、一定不変の識別子を用いて相手コンピュータと通信を行うことができ、例えばTCPコネクションのような論理通信路を移動の前後で維持することができることであると定義することができる。インターネットにおいて、移動透過な通信ができないのは、IPアドレスが持つアドレスと識別子という二重性のためである。

【0019】上記移動透過性を実現するために、具体的には、位置指示子であるIPアドレスに加えて、各ホストに固有の識別子としてVIPアドレスを導入する。

【0020】VIPアドレスとIPアドレスは、同一のフォーマットを有しており、それだけではどちらであるかを区別することができない。これは、オペレーティングシステムの仮想記憶システムにおける仮想アドレスと物理アドレスの関係に対応づけることができる。

【0021】VIPアドレスからIPアドレスへのマッ

ピングを効率よく行うために、VIP層でAMT（Address Mapping Table）と呼ばれるキャッシュを持つようにする。以下では、AMTを構成するデータ単位のことをAMTエントリと呼ぶことにする。AMTエントリは、VIPアドレス、IPアドレス、バージョン番号、その他の管理情報から構成される。

【0022】移動コンピュータ（例えば、図1の移動ホスト24）が送信するパケットのヘッダには、送信コンピュータのVIPアドレス（図4の送信ホスト識別子に対応する）と、IPアドレス（図4の送信ホストアドレスに対応する）が含まれている。従って、移動コンピュータから所定のネットワーク内の所定のコンピュータ（受信コンピュータ）に向けてパケットが送信されたとき、このパケットが受信コンピュータに到達するまでに経由するルータ、および最終的には受信コンピュータにより、そのパケットのヘッダに含まれる送信コンピュータのVIPアドレスとIPアドレスが読み取られ、それに基づいてAMTエントリが作成される。

【0023】このようにして、原則として移動コンピュータが送信したパケットの経路に沿って、AMTエントリが拡散していく。

【0024】VIPアドレスは、位置に依存しない番号であるため、自分以外の他のコンピュータのVIPアドレスを偽ること（他のコンピュータになりすますこと）は容易である。すなわち、送信ホスト識別子に他のコンピュータの識別子（VIPアドレス）を設定し、所定の受信コンピュータにこのパケットを送信することは容易である。これにより、受信コンピュータは、VIPアドレスに対応する他のコンピュータからのパケットを受信したものと認識する。

【0025】そこで、このVIPに新たに認証機構を導入し、不正なコンピュータによる他のコンピュータへのなりすましを防止することを考える。

【0026】そのために、ここでは、Keyed MD（Message Digest）5と呼ばれる方式を用いるものとする。MD5とは、一種のチェックサム計算法であり、任意長のデータから、16オクテット（128ビット）のデータ（MD）を生成する。MD5による演算結果が特定の値になるようなデータを生成することは非常に困難であるとされるため、MD5は通常、改竄防止に使用される。

【0027】Keyed MDでは、送信側（送信コンピュータ）と受信側（受信コンピュータ）で秘密鍵（Secret Key）を共有する。送信側ではデータに秘密鍵を付加したのについてMD5を計算し、計算結果をデータに付加して送信する。一方、受信側では、受信したデータに秘密鍵を付加してMD5を計算し、その計算結果を受信したデータに付加された計算結果と比較する。両者が一致すれば通信途中に改竄が行われていないことがわかると同時に、送信側と受信側が秘密鍵を共有している

こともわかる。従って、第3者が秘密鍵を知らないとは仮定すると、受信者は送信者が「本物」であると認証することができる。

【0028】例えば、送信コンピュータは自分のVIPアドレス、IPアドレス、アドレスバージョン、AMTエントリ保持時間、およびタイムスタンプ等の合計20オクテット(160ビット)のデータに、128ビット(16オクテット)の秘密鍵を付加してMD5の計算を行うようにすることができる。

【0029】また、移動コンピュータ(送信コンピュータ)と移動コンピュータの属するネットワークのファイアウォールで秘密鍵を共有するようにし、ファイアウォールが移動コンピュータが本当に自組織に属していると確認することができたときのみ、ファイアウォールが移動コンピュータからのパケットを外側から内側へ中継するようにすることができる。

【0030】図1は、本発明の通信システムを適用したネットワークの構成例を示している。この例の場合、ある組織のネットワーク(Local area networks in an organization)21は、ファイアウォール(FW)300を介して広域ネットワーク(Wide area network)(例えばインターネット)23に接続されている。また、ネットワーク21には、ホスト(H)25が接続されている。ここでは、各ホストは、仮想インターネットプロトコル(VIP: Virtual Internet Protocol)に基づいて、通信を行うものとする。

【0031】図2は、図1に示した移動ホスト(MH: Mobile Host)24の構成例を示している。記憶部24aは、秘密鍵(Secret Key)を記憶するようになっている。演算部24bは、例えば、一種のチェックサムの演算方法(例えば、MD(Message-Digest)5)を記憶し、記憶部24aに記憶された秘密鍵と、送信すべきパケットのヘッダ内の情報に基づいて、ヘッダ内の情報が本物であるか否かの認証をするためのチェックサム(送信ホスト認証子)を演算するようになっている。また、送受信部24cは、演算部24bによって演算された送信ホスト認証子をパケットのヘッダに含めて送信したり、送られてきたパケットを受信するようになっている。

【0032】図3は、図1に示したファイアウォール300の構成例を示すブロック図である。このファイアウォール300においては、図10に示した従来のファイアウォール200において、受信したパケットのパケットヘッダ内の情報が本物であるか否かを認証する認証器(Authenticator)31をさらに設けるようにしている。

【0033】認証器31は、移動ホスト24が有するものと同一の秘密鍵(Secret Key)、および一種のチェックサムの演算方法(例えば、MD5)を記憶し、後述するように、ネットワークインタフェース1a乃至1cの

所定のものを介して受信したパケットのパケットヘッダ内の情報が本物であるか否かを認証するようになっている。また、この場合、パケット選別器11は、認証器31がパケットヘッダ内の情報が本物であると認証したパケットだけを、経路表3に基づいて決定したネットワークインタフェース1a乃至1cのいずれかを介して、ネットワーク21に中継するようになっている。

【0034】その他の構成は、図10を参照して上述した場合と同様であるので、ここではその説明は省略する。

【0035】例えば、ある組織のネットワーク21に属している移動ホスト24が、この組織のネットワーク21を出て、広域ネットワーク23に接続し、移動ホスト24からこの移動ホスト24が属しているネットワーク21内のホスト25へパケットを送信した場合を考える。その際、移動ホスト24は、送信ホスト認証子を演算し、それをパケットのヘッダに含める。

【0036】また、このとき、移動ホスト24とファイアウォール300は、予め所定の秘密鍵(Ks)をそれぞれ記憶し、共有するようにする。この秘密鍵は、例えば128ビット程度のデータとすることができる。

【0037】また、ここで送信されるパケットは、例えば図4に示したようなパケットフォーマットを有している。すなわち、パケットヘッダ部とデータとからなり、パケットヘッダ部はさらに、送信ホストアドレス(Source Address)(IPアドレス)、送信ホスト識別子(Source Identifier)(VIPアドレス)、送信ホストアドレスバージョン(Source Address Version)、タイムスタンプ(Timestamp)、送信ホスト認証子(Source Host Authenticator)、受信ホストアドレス(Destination Address)(IPアドレス)、受信ホスト識別子(Destination Identifier)(VIPアドレス)、および受信ホストアドレスバージョン(Destination Address Version)の各フィールドより構成されている。

【0038】ここで、送信ホスト認証子は、例えば、次のようにして計算することができる。すなわち、送信ホストアドレス、送信ホスト識別子、送信ホストアドレスバージョン、およびタイムスタンプの各フィールド内のデータに秘密鍵(Ks)を連結して得られたデータに、例えば、MD5(Message Digest 5)のようなアルゴリズムに基づいて、一種のチェックサムを計算することにより得ることができる。このMD5は、任意長のデータから、16バイトのチェックサムを生成するものである。

【0039】また、上記MD5の他に、次のようなアルゴリズム、例えば、DES(Data Encryption Standard)(National Bureau of Standards FIPS Publication 46, 1977)、FEAL(Fast Encryption ALgorithm)(S. Miyaguchi, The FEAL cipher family, Lecture Notes in Computer Science, 537(1991), pp627-638. (Advances in Cryptology - CRYPTO '90))のような暗号化

アルゴリズム、あるいはMD4 (Message Digest algorithm) (R.L.Rivest. The MD4 message digest algorithm. Lecture Notes in Computer Science, 537(1001), 303-311. (Advances in Cryptology - CRYPTO '90)) や SHA (Secure Hash Standard) (SecureHash Standard. National Bureau of Standards FIPS Publication 180, 1993) のようなメッセージダイジェストアルゴリズムを使用することができる。なお、DES、FEALに関しては、「辻井、笠原、「暗号と情報セキュリティ」、1993年7月」に詳しい。

【0040】次に、図5に示したフローチャートを参照して、移動ホスト24が、自組織のネットワーク21から出て、広域ネットワーク23に接続し、ホスト25に対して所定のパケットの送信を行った場合のファイアウォール300の動作について説明する。

【0041】移動ホスト24より送信されたパケットは、まずファイアウォール300に到達し、ステップS1においてこのパケットが、例えばネットワークインタフェース1a (図3) に入力される。すなわち、この場合、ファイアウォール300は、ネットワークインタフェース1aを介して広域ネットワーク23と接続されているものとする。

【0042】ファイアウォール300のネットワークインタフェース1aに入力されたパケットは、ステップS2において、経路表3により、中継可能なパケットであるか否かが判定される。例えば、ファイアウォール300に接続されたネットワーク、この場合、ネットワーク21に、ネットワークインタフェース1aを介して入力したパケットのパケットヘッダに含まれる受信ホストアドレスに対応するホストが存在するか否かが判定される。

【0043】その結果、ネットワーク21内に、パケットヘッダに含まれる受信ホストアドレスに対応するホストが存在しないと判定された場合、ステップS3に進み、このパケットが廃棄される。その後、ステップS1に戻り、ステップS1より以降の処理が繰り返し実行される。一方、パケットヘッダに含まれる受信ホストアドレスに対応するホストが、ネットワーク21内に存在すると判定された場合、ステップS4に進む。

【0044】ステップS4においては、パケット選別器11により、中継してよいパケットであるか否かが判定される。例えば、ある組織のネットワーク21に属する移動ホストからのパケットであるか否かが判定される。中継してよいパケットではないと判定された場合、ステップS5に進み、このパケットは廃棄される。その後、ステップS1に戻り、ステップS1より以降の処理が繰り返し実行される。一方、中継してよいパケットであると判定された場合、ステップS6に進む。

【0045】ステップS6においては、ファイアウォール300を構成する認証器31により、ステップS1に

おいて入力されたパケットのパケットヘッダの情報が本物であるか否かが判定される。すなわち、認証器31は、移動ホスト24が有する秘密鍵および一種のチェックサムの演算方法 (例えばMD5) と同一のものを有しており、この秘密鍵とパケットを構成するパケットヘッダの内容から、上述した移動ホスト24において行われた場合と同様にして、再度、送信ホスト認証子が独自に計算される。

【0046】そして、この計算によって得られたチェックサムとしての送信ホスト認証子と、ネットワークインタフェース1aを介して入力されたパケットのパケットヘッダの中に含まれる送信ホスト認証子が比較される。そして、両者が一致するか否かを判定することによって、入力されたパケットのパケットヘッダ内の情報が本物であるか否かの認証が行われる。

【0047】すなわち、この計算によって得られた送信ホスト認証子と、入力されたパケットヘッダの中に含まれる送信ホスト認証子が一致しない場合、このパケットのパケットヘッダ内の情報は本物ではないと認証され、ステップS7に進み、このパケットは廃棄される。その後、ステップS1に戻り、ステップS1以降の処理が繰り返し実行される。

【0048】一方、この計算によって得られた送信ホスト認証子と、入力されたパケットのパケットヘッダの中に含まれる送信ホスト認証子が一致した場合、このパケットのパケットヘッダの情報は本物である、すなわち、移動ホスト24から送信されてきたパケットであると認証され、ステップS8に進む。

【0049】ステップS8においては、このパケットを中継するための処理が行われる。すなわち、経路表3に基づいて、このパケットの受信ホストアドレスに対応するホストが存在するネットワークへのルート (経路) が決定される。次に、それに基づいて、送信ネットワークインタフェース決定器2により、ネットワークインタフェース1a乃至1cのうち、このパケットを送信すべきネットワークへの経路上にある、例えば、ネットワークインタフェース1bが決定される。すなわち、この場合、ファイアウォール300とネットワーク21とは、ネットワークインタフェース1bを介して接続されているものとする。

【0050】次に、ステップS9において、ネットワークインタフェース1bを介して、このパケットが出力され、ネットワーク21に中継される。

【0051】その後、ステップS1に戻り、ステップS1より以降の処理が繰り返し実行される。

【0052】このように、ファイアウォール300は、自組織のネットワーク21に属する移動ホスト24からのパケットだけを、自組織のネットワーク21に選択的に中継することができるので、通信におけるセキュリティの向上を図ることができる。

【0053】図6は、本発明の通信システムを適用したネットワークの他の実施の形態の構成例を示している。同図に示すように、ある組織（自組織）41は、メールサーバ42とFTP（File Transfer Protocol）サーバ43を有しており、ファイアウォール45を介してインターネット46に接続されている。また、自組織41に属するノートPC（パーソナルコンピュータ）44は、自組織41を離れて、インターネット46にモデムを介して接続されている。

【0054】次に、図7および図8を参照して、図6に示したように、自組織41に属するノートPC44が、この組織外でインターネット46に接続し、自組織41内のメールサーバ42にアクセスする場合について説明する。なお、FTPサーバ43にアクセスする場合も基本的にメールサーバ42にアクセスする場合と同様である。

【0055】ここでは、ノートPC44には、VIPが実装されており、ファイアウォール45は、ノートPC44のホームルータも兼ねているものとする。また、ファイアウォール45は、内側から外側へ送信されるパケットに関しては無条件に中継するものとする。そして、ファイアウォール45とノートPC44は秘密鍵を共有し、所定の計算方法（例えば、MD5）をそれぞれ記憶しているものとする。

【0056】図7は、ノートPC44の動作手順を表すフローチャートであり、図8は、ファイアウォール45の動作手順を表すフローチャートである。

【0057】まず、図7のステップS11において、例えば、ユーザはノートPC44を用いて、出張先のホテルからモデムおよび電話回線を介してダイヤルアップにより、インターネットプロバイダに接続する。次に、ステップS12において、ノートPC44は、インターネットプロバイダからIPアドレスの割り当てを受ける。すなわち、ノートPC44のIPアドレスは、ノートPC44が移動することによって変化することになる。しかしながら、ノートPC44のVIPアドレスは変化しない。このようにして、ある組織41に属するノートPC44が、組織外の所定の地点でインターネット46に接続する。

【0058】ステップS13においては、ノートPC44は、コントロールパケットにより、自分のVIPアドレスとIPアドレスをファイアウォール（ホームルータ）45に送信する。

【0059】ノートPC44から送信されてきたこのコントロールパケットのヘッダには、ノートPC44の認証データ（図4の送信ホスト認証子に対応する）がヘッダ情報として含まれているので、ファイアウォール45は、図1乃至図5を参照して上述した場合と同様に、ノートPC44が本物であるか否かを認証することができる。

【0060】ファイアウォール45は、図8のステップS21において、ノートPC44からのコントロールパケットを受信すると、ステップS22に進み、コントロールパケットに含まれるヘッダの中の送信ホスト認証子および他のヘッダ情報に基づいて、ノートPC44の認証を行う。そして、ステップS23において、ファイアウォール45により、ステップS22における認証の結果に基づいて、ノートPC44が本物であるか否かが判定される。すなわち、ノートPC44が本当に自組織41に属するコンピュータであるか否かが判定される。ノートPC44が本物ではないと判定された場合、ステップS29において、このパケットが廃棄された後、処理を終了する。一方、ノートPC44が本物であると判定された場合、ステップS24に進み、ノートPC44から送信されてきたコントロールパケットのヘッダに含まれるノートPC44のVIPアドレスとIPアドレスの関係がAMTに登録される。

【0061】従って、それ以降、ファイアウォール41は、AMTによってノートPC44のVIPアドレスをIPアドレスに変換することができるようになる。

【0062】次に、ユーザが自組織41内のメールサーバ42にアクセスし、自分宛のメール（電子メール）を読む場合、ノートPC44は、図7のステップS14において、メールを読むために、自分宛のメールの送信を要求する所定のVIPパケットを自組織41のメールサーバ42に向けて送信する。このパケットには、ノートPC44の認証データ（図4の送信ホスト認証子に対応する）が含まれている。

【0063】ファイアウォール45は、図8のステップS25において、ノートPC44からメールサーバ42に向けて送信されたVIPパケットを受信すると、ステップS26に進み、ノートPC44からのVIPパケットのヘッダに含まれる送信ホスト認証子とその他のヘッダ情報に基づいて、ノートPC44の認証を行う。次に、その認証結果に基づいて、ステップS27において、ファイアウォール45によりノートPC44が本物であるか否かが判定される。すなわち、ノートPC44が本当に自組織41に属するコンピュータであるか否かが判定される。ノートPC44が本物ではないと判定された場合、ステップS29において、このパケットが廃棄された後、処理を終了する。一方、ノートPC44が本物であると判定された場合、ステップS28に進み、そのVIPパケットが自組織41に中継される。

【0064】これにより、VIPパケットは、メールサーバ42に到達し、メールサーバ42により、VIPパケットによるユーザからの要求が処理される。この場合、ユーザ宛のメールがあればそれを含めた応答パケットをノートPC44に送信する。ユーザ宛のメールがなければ、そのことを表す応答パケットをノートPC44に送信する。このとき、上述したように、VIPが提供

する移動透過な通信機能（移動透過性）により、ノートPC44の位置に拘らず、この応答パケットは、ファイアウォール45、インターネット46を介して伝送され、ノートPC44に到達する。

【0065】すなわち、上記応答パケットには、ノートPC44のVIPアドレスが含まれており、このVIPアドレスは、ファイアウォール45において、AMTに基づいてIPアドレスに変換される。そして、応答パケットは、このIPアドレスに基づいて、インターネット46を介してノートPC44に伝送される。

【0066】ノートPC44においては、図7のステップS15において、メールサーバ42からの応答パケットが受信される。そして、応答パケットにユーザ宛のメールが含まれる場合、それが画面に表示される。また、応答パケットにユーザ宛のメールが含まれていない場合、ユーザ宛のメールがないことを示す所定のメッセージが画面に表示される。

【0067】このようにして、ユーザは、例えば出張先のように任意の場所からファイアウォール45を越えて自組織41の内部のメールサーバ42にアクセスし、自分宛のメールを読むことが可能となる。同様に、ユーザは、自組織41内のメールサーバ42にメールを送信することができる。その場合、メールを含んだVIPパケットをメールサーバ宛に送信することになる。

【0068】最近では、ノートブック型のコンピュータを持ち歩き、行く先々で自組織のメールサーバにアクセスし、メールの読み書きをしているユーザも多い。上述したように、VIPではファイアウォールが移動コンピュータからのパケットに基づいて移動コンピュータの認証を行い、自組織に属する移動コンピュータからのパケットを安全に自組織内へ中継することができる。これにより、ユーザは、ファイアウォールの存在を意識することなく、外部からインターネット等を介して、ファイアウォールを越えて自組織内のメールサーバにアクセスし、メールの読み書きを行うことができる。

【0069】なお、上記実施の形態においては、ユーザがノートPC44を用いてメールサーバ42にアクセスする場合について説明したが、メールサーバ42にアクセスする場合と基本的に同様の手順で、ユーザはノートPC44を用いてファイアウォール45を越えて自組織41のFTPサーバ43にアクセスし、FTPサーバ43とノートPC44の間でファイルの転送を行うことができる。従って、ユーザは、例えば出張先のように任意の場所からファイアウォール45を越えて自組織41のFTPサーバ43にアクセスし、所望のファイルを取り寄せることが可能となる。

【0070】また、上記実施の形態においては、送信ホスト認証子を求めるためにMD5を用いるようにしたが、これに限定されるものではなく、他の方法を用いるようにすることも可能である。

【0071】また、上記実施の形態においては、仮想インターネットプロトコルに基づいてパケットが送受信されるネットワークに本発明を適用する場合について説明したが、他のプロトコルに基づいたネットワークに本発明を適用することも可能である。

【0072】

【発明の効果】請求項1に記載の通信システムによれば、送信局において、第1の演算手段により、第1の記憶手段に記憶された鍵情報と、受信局に送信すべきパケットのヘッダ情報に基づいて、記憶している演算方法に従って第1の認証情報が演算され、送信手段により、第1の演算手段によって演算された第1の認証情報がパケットのヘッダ情報に含められて送信される。また、通信装置において、第2の演算手段により、第2の記憶手段に記憶された鍵情報と、送信局からのパケットのヘッダ情報に基づいて、記憶している演算方法に従って第2の認証情報が演算され、比較手段により、送信局からのパケットのヘッダ情報に含まれる第1の認証情報と、第2の認証情報とが比較され、この比較結果に基づいて、決定手段により、パケットを第2のネットワークに中継するか否かが決定されるようにしたので、通信装置が記憶している鍵情報および演算方法と同一のものを記憶している送信局からのパケットのみを選択的に中継することができるので、通信のセキュリティを向上させることが可能となる。

【0073】請求項6に記載の通信装置によれば、認証手段により、ネットワークインタフェースを介して受信した送信局からのパケットに含まれるヘッダ情報が本物であるか否かが認証され、制御手段により、認証手段によってパケットに含まれるヘッダ情報が本物であると認証されたとき、パケットが中継されるよう制御されるようにしたので、ヘッダ情報が本物である場合にだけ、そのパケットを中継するようになすことができ、通信のセキュリティを向上させることができる。

【図面の簡単な説明】

【図1】本発明の通信システムを適用したネットワークの一実施の形態の構成例を示す図である。

【図2】図1の移動ホストの構成例を示すブロック図である。

【図3】図1のファイアウォールの構成例を示すブロック図である。

【図4】パケットフォーマットおよび送信ホスト認証子の演算方法を示す図である。

【図5】図3のファイアウォールの動作を説明するためのフローチャートである。

【図6】本発明の通信システムを適用したネットワークの他の実施の形態の構成例を示す図である。

【図7】外部からメールサーバ42にアクセスするときのノートPC44の動作手順を示すフローチャートである。

【図8】ノートPC 44がメールサーバ42にアクセスするときのファイアウォール45の動作手順を示すフローチャートである。

【図9】従来のルータの構成例を示すブロック図である。

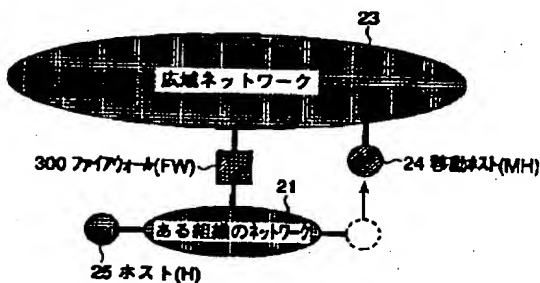
【図10】従来のファイアウォールの構成例を示すブロック図である。

【符号の説明】

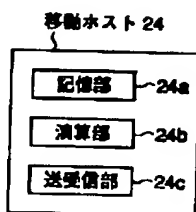
1 a, 1 b, 1 c ネットワークインタフェース, 2

送信ネットワークインタフェース決定器, 3 経路表, 11 パケット選別器, 21 ある組織のネットワーク, 23 広域ネットワーク, 24 移動ホスト, 24 a 記憶部, 24 b 演算部, 24 c 送受信部, 25 ホスト, 41 自組織, 42 メールサーバ, 43 FTPサーバ, 44 ノートPC, 45 ファイアウォール (ホームルータ), 46 インターネット, 100 ルータ, 200, 300 ファイアウォール

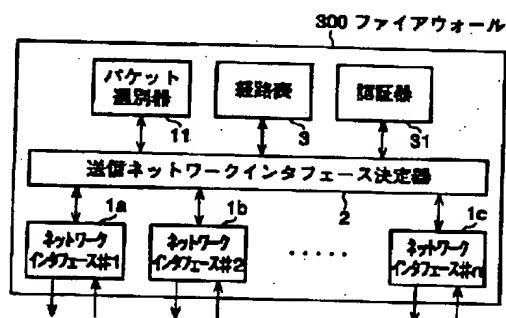
【図1】



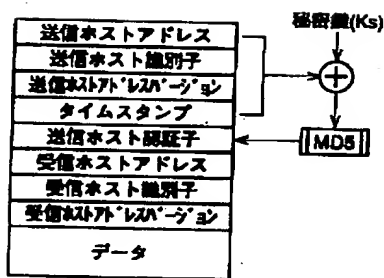
【図2】



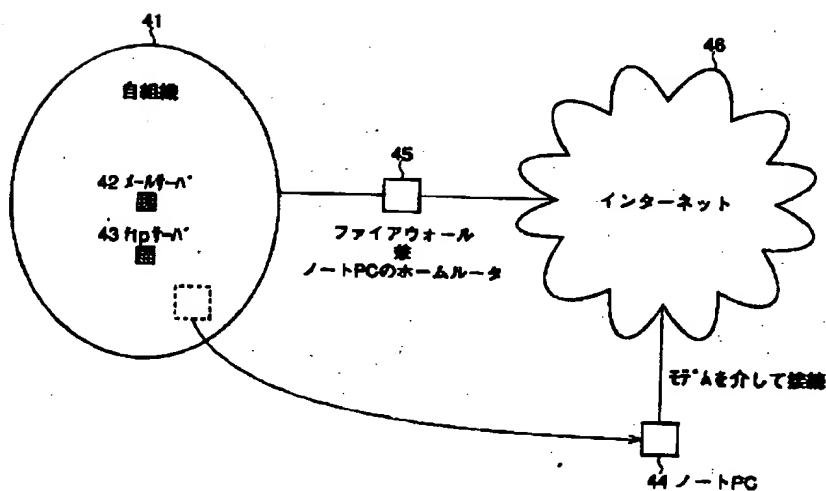
【図3】



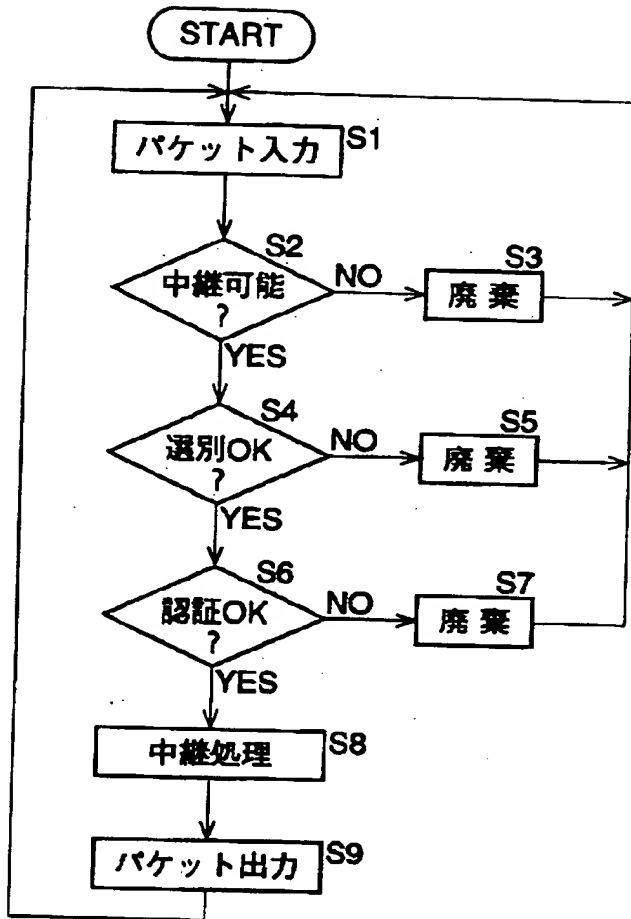
【図4】



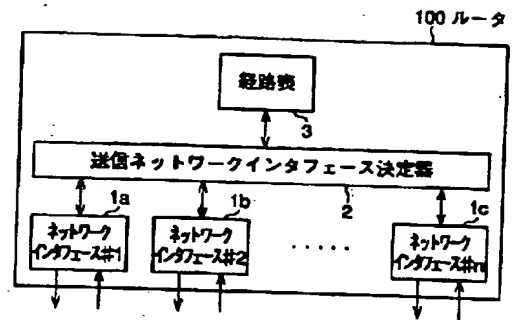
【図6】



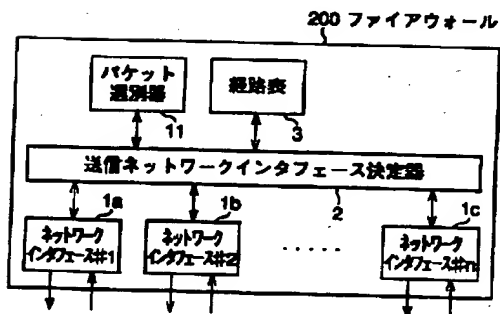
【図5】



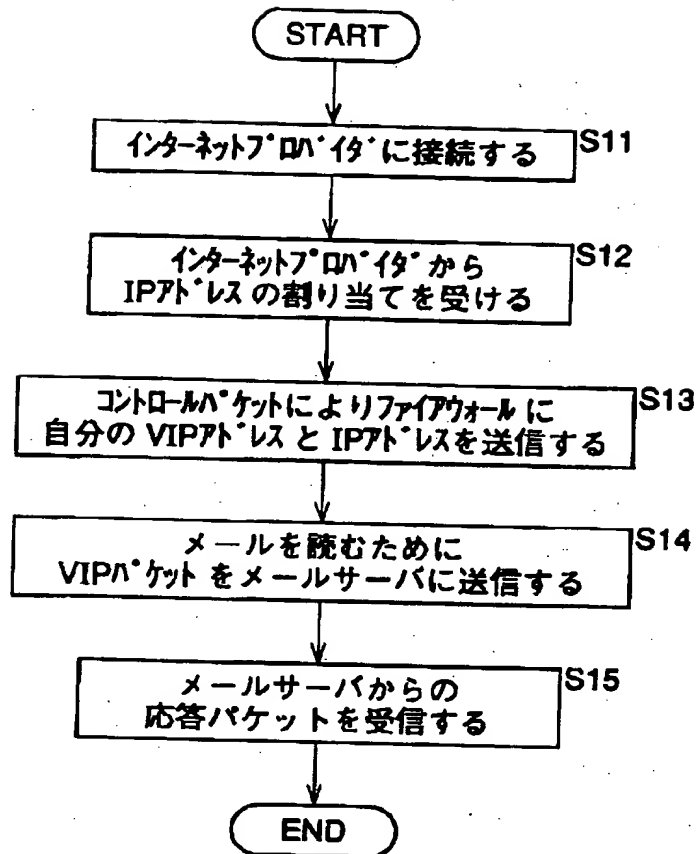
【図9】



【図10】

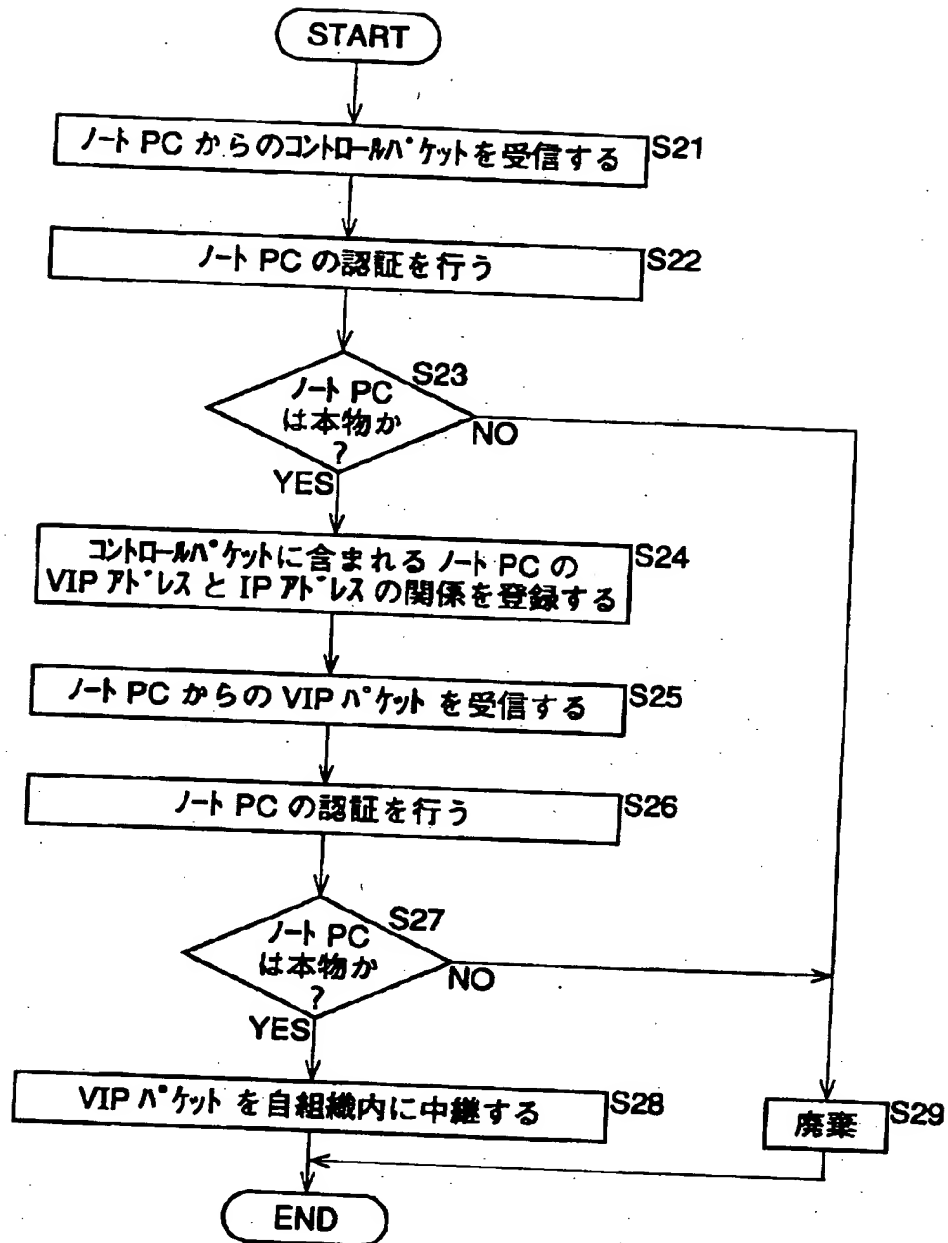


【図 7】



ノート PC の動作手順

【図8】



ファイアウォールの動作手順